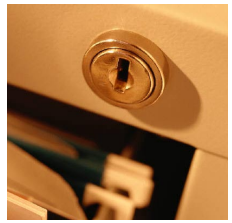
MARSH



HIPAA PRIVACY

Marsh & McLennan Companies

Presented By: Marsh USA Inc.
For: Washington Fire Commissioners Association
October 24, 2003

HIPAA ADMINISTRATIVE SIMPLIFICATION
Privacy, EDI/TCS, Security

EFFECTIVE DATES FOR HEALTH PLANS:

	EFFECTIVE	EFFECTIVE (Small Plans*)	Enforcement Agency
Privacy	4 / 14 / 2003	4 / 14 / 2004	OCR
EDI	10 / 16 / 2002	10 / 16 / 2003**	CMS
Security	4 / 21 / 2005	4 / 21 / 2006	CMS

* Small Plans: Health Plans with less than $5 million in annual receipts
-For Insured Plans, “receipts” are premiums for last full fiscal year
-For Self-Funded Plans, “receipts” are the total amount paid for health care claims for last full fiscal year

** Includes those Plans that filed (by 10/15/02) for one-year extension

HIPAA PRIVACY (HEALTH PLANS) THE BIG PICTURE

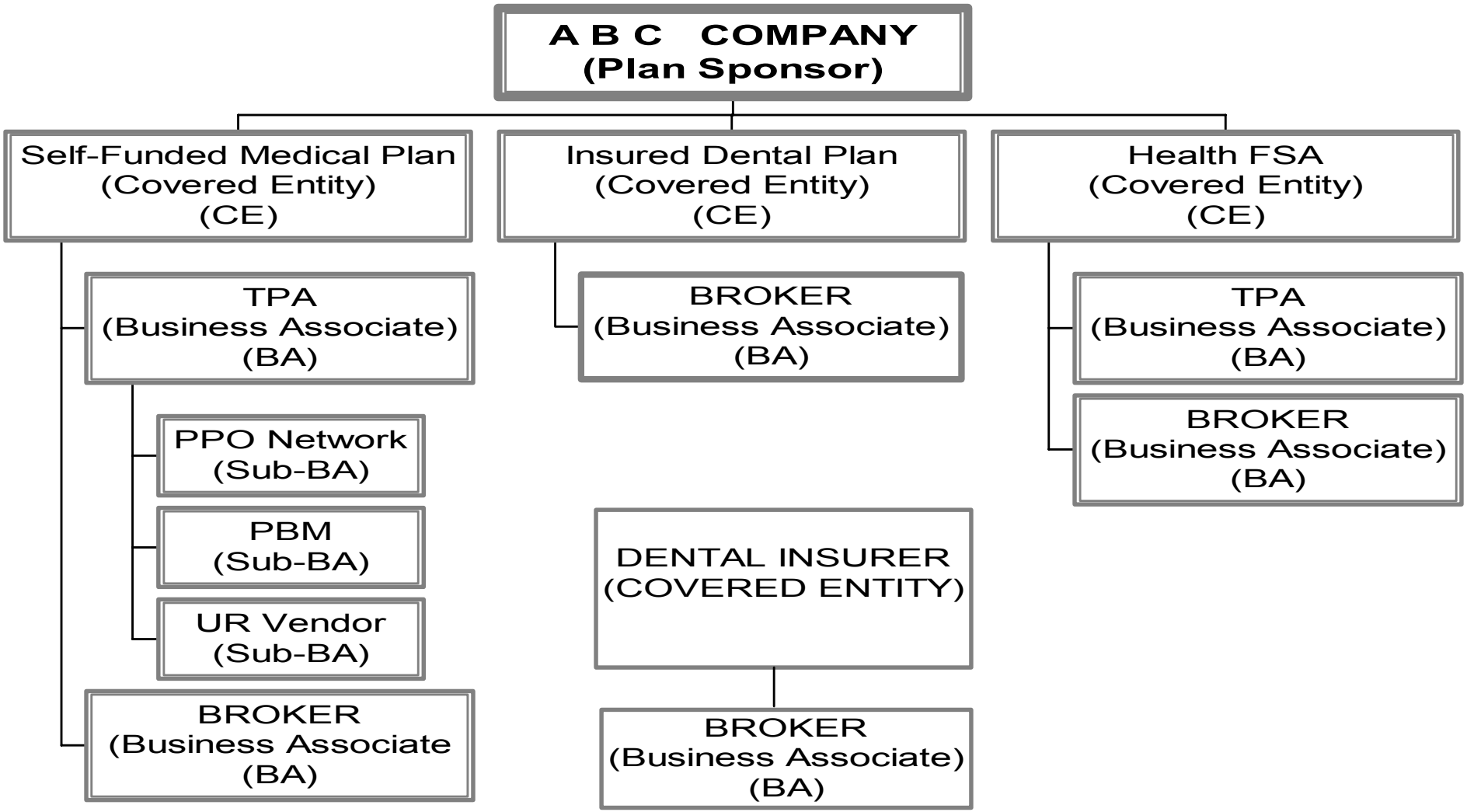
A Covered Entity (Health Plan, Healthcare Provider, Healthcare Clearinghouse) :

- **Cannot use or disclose protected health information (PHI)** without written authorization of the individual to whom the PHI relates, except as permitted or required under the regulations.
  - Permitted uses and disclosures include: Treatment, Payment, and Health Care Operations (TPO).

The Health Plan is the Covered Entity (CE), which includes:

- A group (or individual) health plan that provides or pays the cost of medical care
- *Examples* of Health Plans (includes Insured Plans and Self-Funded Plans):
  - Medical, Prescription Drug, Vision, and/or Dental plans
  - Health Care Flexible Spending Accounts and Health Reimbursement Accounts
  - Employee Assistance Programs (EAPs)
- Insurers are also Health Plans
- NOTE: Plans that are self-funded AND self-administered with less than 50 Participants are exempt.

HIPAA PRIVACY (HEALTH PLANS)
THE BIG PICTURE



HIPAA PRIVACY (HEALTH PLANS) THE BIG PICTURE

WHAT INFORMATION IS SUBJECT TO HIPAA PRIVACY?

- **Protected Health Information (PHI)**, which is:
  - "Individually Identifiable Health Information" that is maintained or transmitted by a Covered Entity
    - This includes enrollment information once it is transferred to the Health Plan
- **PHI is not:**
  - Information that is specifically excluded in the regulations, for example:
    - Education records
    - Employment records that are created or maintained by the employer
      - Watch for the dual-role employers have as employer and as plan sponsor
      - Employment records are not defined by regulations, but could include records related to occupational injury, disability insurance eligibility, sick leave reports, drug screening, fitness-for-duty tests, etc.
  - "De-identified Health Information" which is information that is de-identified by either a professional statistical analysis; or, by removing 18 specific identifiers

HIPAA PRIVACY (HEALTH PLANS) WHAT ARE THE RULES?

1. PROTECTED HEALTH INFORMATION (PHI) USE AND DISCLOSURE

A. Rules For: Who has access to and uses PHI; How PHI is disclosed; Other Rules

- Permissible uses by the **Health Plan** are "Payment" and "Health Care Operations"

B. Rules For: Sharing PHI with the Plan Sponsor (from the Health Plan)

- Generally, the Health Plan **CANNOT** share PHI with the Plan Sponsor, except:
  - can disclose "Summary Health Information", but only for the purpose of obtaining insurance bids and/or for modifying, amending, or terminating the Plan
  - can disclose "Enrollment / Disenrollment" information
  - can disclose PHI for purposes of "Plan Administration Functions", but only if:
    - the Plan Document is amended to describe the permitted and required uses and disclosures of PHI by the Plan Sponsor; and
    - the Plan Sponsor maintains firewalls; and
    - the Plan Sponsor certifies that the Plan Document has been amended and firewalls have been established and agrees to the restrictions
  - can disclose PHI with the individual's authorization

HIPAA PRIVACY (HEALTH PLANS) WHAT ARE THE RULES?

2. ADMINISTRATIVE SAFEGUARDS

A Covered Entity (the Health Plan) must:

- Designate a Privacy Official who is responsible for developing & implementing policies and procedures & a Contact Person for receiving complaints & explaining Privacy Notice
- Develop and implement policies and procedures to comply with Privacy rules
- Train workforce regarding privacy policies & procedures
- Create a process for individuals to lodge complaints and system for handling complaints
- Develop written disciplinary policies & develop appropriate sanctions for violations
- Mitigate any harmful effect that resulted from improper use or disclosure of PHI
- Establish safeguards for protecting the privacy of PHI to include administrative, technical and physical safeguards
- Refrain from intimidating/retaliating against individuals (or others) who exercise their rights, file a complaint, participate in an investigation, oppose any improper practice
- Not require an individual to waive their rights

HIPAA PRIVACY (HEALTH PLANS) WHAT ARE THE RULES?

3. INDIVIDUALS' RIGHTS

Individuals have the right to:

- Inspect / make copy of their PHI (as contained in their "Designated Records Set - DRS")
- Amend / correct their incorrect or incomplete PHI (as contained in their "DRS")
- Receive an accounting of non-routine PHI disclosures made by the Health Plan
  - does not include disclosures for TPO (treatment, payment, or healthcare operations) or pursuant to the individual's authorization
- Request that their PHI be communicated by alternative methods or to alternative locations
- Request additional restrictions on the use / disclosure of their PHI (Health Plan can deny)
- Receive a Privacy Notice

HIPAA PRIVACY (HEALTH PLANS) WHERE TO START?

Initial Steps:

1. Identify each of your Health Plan(s) that are subject to HIPAA Privacy
   - These Health Plans will be Covered Entities
2. Identify the Business Associates (BA) for each Health Plan
3. Note whether the Health Plan(s) is:
   - Insured?
   - Self-Funded?
   - Self-Funded and Self-Administered with fewer than 50 participants?
4. If the Health Plan is insured, determine whether you (the Plan Sponsor) will be:
   - Receiving / using PHI from the Health Plan (other than "Summary Health Information" or "Enrollment/Disenrollment" information)
5. Identify employees (or classes of employees) of the Plan Sponsor with access to each Health Plan's health information and determine why they have PHI access
6. Identify the "flow" of PHI between: The Health Plan(s), the Plan Sponsor's employees, and the Business Associate(s)

HIPAA PRIVACY (HEALTH PLANS) WHERE TO START?

7A. Where to Start For: Insured Plans - Where Plan Sponsor has NO access to PHI

Plan Sponsor can still receive Summary Health Information (for limited purposes) and Enrollment/Disenrollment information.

- The **Health Plan**:
  - Must follow the Insurer's "rules"
  - Must refrain from intimidating or retaliating against individuals (or others) that exercise their rights, file a complaint, participate in an investigation, or oppose any improper practice
  - Cannot require individuals to waive their rights
- The Insurer must fully comply with HIPAA Privacy Rules
  - This includes sending their Privacy Notice to enrollees

HIPAA PRIVACY (HEALTH PLANS) WHERE TO START?

7B. Where to Start For: Insured Plans - Where Plan Sponsor HAS access to PHI

- The **Health Plan must**:
  - Comply with the Administrative Safeguards
  - Provide for individuals' rights
  - Prepare Privacy Notice (BUT only need to provide to enrollees upon request)
  - Amend the Plan Document to establish the permitted and required uses and disclosures of PHI by the Plan Sponsor
  - Receive the Plan Sponsor's Certification that (1) the Plan has been amended; and (2) that firewalls are in place to protect disclosed PHI
  - Enter into Business Associate Agreements (BAAs)
- The **Plan Sponsor must**:
  - Comply with the plan document (amendment) requirements
  - Comply with the firewall requirements
  - Provide Certification to the Health Plan that these requirements are satisfied
- The Insurer must fully comply with HIPAA Privacy rules (including sending Notices)

HIPAA PRIVACY (HEALTH PLANS) WHERE TO START?

7C. Where to Start For: Self-Funded Plans

- The **Health Plan must**:
  - Comply with the Administrative Safeguards
  - Provide for individuals' rights
  - Prepare Privacy Notice -- and deliver Privacy Notice to enrollees
  - Amend the Plan Document to establish the permitted and required uses and disclosures of PHI by the Plan Sponsor
  - Receive the Plan Sponsor's Certification that (1) the Plan has been amended; and (2) that firewalls are in place to protect disclosed PHI
  - Enter into Business Associate Agreements (BAAs)
- The **Plan Sponsor must**:
  - Comply with the plan document (amendment) requirements
  - Comply with the firewall requirements
  - Provide Certification to the Health Plan that these requirements are satisfied

HIPAA ENFORCEMENT / PENALTIES

- PRIVACY: Enforced by HHS Office for Civil Rights (OCR)
- EDI & SECURITY: Enforced by HHS Centers for Medicare & Medicaid Services (CMS)

BOTH OCR and CMS have indicated that their enforcement activities will largely be complaint-driven and that their goal is to seek voluntary compliance through technical assistance. **. . . . . At least initially . . . . .**

- CIVIL PENALTIES (HHS): $100 / person / violation (up to $25,000 / calendar year for identical violations). May not be imposed:
  - if HHS is satisfied the person did not know / would not know by applying reasonable diligence
  - if due to reasonable cause and not willful neglect AND corrected within certain time period (generally 30 days from date violation is discovered)
- CRIMINAL PENALTIES:
  - for wrongful disclosure of PHI: Up to $50,000 and 1 year in jail
  - Intentional sale, transfer or use of PHI for personal gain or commercial advantage: $250,000 and 10 years in jail

HIPAA DEFINITIONS

De-identified Health Information:

Information that is de-identified by (1) a professional statistical analysis; or, (2) removing the following 18 identifiers:

(1) Name

(2) Geographic subdivisions smaller than a state (except initial 3 digits of zip)

(3) Dates (EXCEPT YEAR) related to the individual (including birth, admission, discharge, death, and for individuals over age 89 -no date- but can aggregate with others over age 89 into one category of “age 90 or older”)

(4) Telephone numbers

(5) Fax numbers

(6) Email addresses

(7) Social Security numbers

(8) Medical record numbers

(9) Health Plan beneficiary numbers

(10) Account numbers

(11) Certificate / license numbers

(12) Vehicle identifiers and serial numbers (including license plate numbers)

(13) Device identifiers and serial numbers

(14) URLs

(15) IP addresses

(16) Biometric identifiers, including finger and voice prints

(17) Full-face photographic images and comparable images

(18) Any other unique identifying number, characteristic, or code

HIPAA DEFINITIONS

Designated Record Set (DRS):

The medical records, billing records, enrollment, payment, claims adjudication, case management, medical management records systems maintained by or for a Health Plan; or, used in whole or in part, by or for the Covered Entity to make decisions about individuals. There are specified retention requirements for DRS.

Electronic Media:

Electronic storage media including

- Telephone voice response, faxback systems; or
- Memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as a magnetic tape or disk, optical disk, or digital memory card; or
- Transmission media used to exchange information already in electronic storage media. Transmission media includes (for example), the internet (wide-open), extranet (using internet technology to like business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.

Enrollment / Disenrollment:

Not defined in Privacy rules, but will follow EDI rules for “Enrollment Standard Transaction”. Examples:

- Whether the individual is participating in the Health Plan
- Whether the individual is enrolled in or disenrolled from a Health Plan option

HIPAA DEFINITIONS

Health Care Operations (from "TPO" - Treatment, Payment & Health Care Operations):

Activities such as:

- Conducting quality assessment and improvement
- Reviewing competence or qualifications of health care professionals, and of health plan performance
- Underwriting, premium rating, other activities relating to the creation, renewal, or replacement of health insurance or health benefits (including excess loss insurance)
- Medical review, legal services, auditing functions

Health Information:

Information (oral or otherwise) that:

- relates to an individual's past, present or future medical condition (physical or mental health); or
- the provision of medical care for that individual; or
- the past, present or future payment for that individual's medical care.

Individually Identifiable Health Information:

- Health Information that identifies the individual to whom it relates -or- could reasonably identify the individual

HIPAA DEFINITIONS

Minimum Necessary:

- Ensuring that PHI is only used, disclosed and received at the minimum level necessary to accomplish the intended purpose of the use, disclosure, or request
- HHS Guidance provides for flexibility to address a CE's unique circumstances
- Incidental Disclosures are permitted (as long as the CE has complied with the Administrative Safeguards and Minimum Necessary rules
- Does not include:
  - Use or disclosure made to the individual
  - Use or disclosure pursuant to an authorization
  - Disclosures or requests to a health care provider for treatment purposes
  - Disclosures to HHS for compliance and enforcement purposes
  - Use or disclosure required by law

Payment (from "TPO" - Treatment, Payment & Health Care Operations):

Health Plan obtains premiums or determines/fulfills its responsibility for provision of benefits under the Health Plan or to obtain or provide reimbursement for health care. Examples:

- eligibility and coverage determinations
- billing, claims management, obtaining payment under excess loss
- review of health care services with respect to medical necessity, coverage under the Plan, appropriateness of care, justification of charges, utilization review activities and retrospective review of services

HIPAA DEFINITIONS

Plan Administrative Functions:

- Includes many of the activities under “Payment” and Health Care Operations”, for example: quality assurance, claims processing, auditing , monitoring
- Does NOT include things such as: activities related to changing or terminating a plan*, soliciting bids*, employment-related functions, activities related to other benefits.

  *This means that a Plan Sponsor can only use Summary Health Information for these purposes

Summary Health Information:

Information that summarizes the Health Plan’s claims history, expenses, or types of claims as long as the information has 18 specific identifiers removed.

- These 18 identifiers are the same 18 identifiers under to define “de-identified health information” except that the geographic subdivisions can be aggregated to the level of a 5-digit zip code.

HIPAA
SOME RESOURCES

GOVERNMENTAL:

For Privacy: OCR (Office of Civil Rights):

www.hhs.gov/ocr/hipaa

For EDI / Security: CMS (Centers for Medicare & Medicaid Services)

www.cms.hhs.gov/hipaa/hipaa2

To Ask HIPAA Questions: CMS Email Box: askhipaa@cms.hhs.gov

CMS HPIAA Hotline: 1-866-282-0659

Free CMS HIPAA Training Webcast

www.eventstreams.com/cms/tm_001

Free HIPAA Roundtable Conference Call

See CMS website for information on the next conference call

Free Listserve for Notification of Proposed or Final Regulations

Send email to subscribe to: listserv@list.nih.gov (see CMS website for instructions)

Free Listserve for HIPAA Announcements, New Tools, Educational Material

http://list.nih.gov (Browse for HIPAA-Outreach-L)

HIPAA
SOME RESOURCES

State Privacy Laws

www.healthprivacy.org

Law Firms

Reference Manuals

EBIA (Employee Benefits Institute of America)	www.ebia.com
Thompson Publishing	www.thompson.com

Web-based Tools

HIPAAnswers	www.hipaanswers.com
Privacy Central	www.privacycentral.net

Other

HIPAAdvisory	www.hipaadvisory.com
WEDI (Workgroup for Electronic Data Interchange)	www.wedi.org